DISA

2004 CUSTOMER PARTNERSHIP CONFERENCE

REALIZING THE NET-CENTRIC VISION

DMZ Technical Brief for DISA Customer Conference

Dan Gahafer
GIG Combat Support
Defense Information Systems Agency

REALIZING THE NET-CENTRIC VISION

Demilitarized Zone (DMZ)

- DMZ is a commercial term coined after the military usage associated with buffer zones between adversaries
- Simple definition is that a DMZ is a buffer network separating a private network from a public network
- Primarily used as a security device

REALIZING THE NET-CENTRIC VISION

IAP vs. DMZ

- Internet Access Points (IAP) are general purpose gateways between the Defense Information System Network (DISN) and the Internet
  - Everything outbound to the Internet and the returns
  - Inbound in accordance with the Ports and Protocols Program
- DMZs are special purpose gateways defined by the services (ports and protocols) they are designed to enable
  - Inbound for specific services and outbound only for the returns
  - Complementary to the Ports and Protocols and IAP Programs

REALIZING THE NET-CENTRIC VISION

DMZ Program

- Addresses Ports and Protocols Program requirements and DoD mandated port closures due to attacks on Web Services
- Implement DMZs to buffer DoD network environment from public networks
- Move system access points to the perimeter(s)
- Create more secure enclaves within the DoD
- Facilitate communications between DoD organizations and non-DoD vendors and partners
- 2 DMZ types in use, Web DMZ and B2B Gateway

REALIZING THE NET-CENTRIC VISION

B2B vs Web DMZ

- Web DMZ
  - Users come from anywhere in the world
  - Users are not authenticated by the DMZ, but may be authenticated by the Web applications
  - DMZ doesn’t require encryption but allows it (https)
  - Developed as a high-availability response (including significant security) to Code Red/NIMDA worms
- B2B Gateway
  - Users access from specific locations
  - System to system access supported
  - All accesses are authenticated
  - DMZ requires IPSEC encryption via Virtual Private Network (VPN)
  - Developed as a security device that is highly available in concert with Ports and Protocols Program guidance

REALIZING THE NET-CENTRIC VISION

Web DMZ Requirements

- Approved mechanism to support critical Ebusiness web servers that must remain accessible from Internet
- Geographic and topological diversity to address Distributed Denial of Service (DDoS) threat
- Sufficient bandwidth to handle DDoS
- Layered security
- Highly available with automatic failover
- Allow from anywhere to select web locations

REALIZING THE NET-CENTRIC VISION

Criticality of Applications

- DISA defers to customers to assess the criticality of DMZ hosting of web based applications
- As an example of how to assess, DLA gathers and uses the following information to evaluate criticality
  - Mission Impact – Provide the impact on the activity's mission if access to the site was cut-off due to port closure. The impact must be directly related to the activity's mission and DLA mission
  - Operating Hours and Scheduled Downtime – Provide the Web site's operating hours and average monthly downtime (scheduled and unscheduled)
  - Number of Users – Over a monthly period, provide the greatest number of users accessing the site and indicate whether the number is planned or actual

REALIZING THE NET-CENTRIC VISION

Web DMZ Chronology

- 3rd QTR 2001, Code Red & Nimda hit - DoD orders closure of inbound HTTP disabling many Web enabled Ebusiness applications
- 3rd QTR 2001, DISA decides upon a DMZ solution to prevent recurrence
- 4th QTR 2001, 1st Web DMZ, DECC Columbus OH
  - Agencies immediately begin migration - DLA, DSCA, MTMC
- 3rd QTR 2002, first app goes production
- 2nd QTR 2003, 2nd Web DMZ, DECC Det San Antonio
- 3rd QTR 2003, 3rd Web DMZ, SMC Montgomery
- 3rd QTR 2003, fully accredited “virtual” DMZ

REALIZING THE NET-CENTRIC VISION

Web DMZ
DISA Technical Solution

- Engineered to provide reliable commercial Internet access
  - To select DoD Web sites and portals
  - Maintains security and integrity of the DISN
- Conforms to the DoD security requirements
  - Outlined in the DoD NIPRNet Ports, Protocol and Services (PPS) Security Technical Implementation Guidance (STIG)
  - The established guidance on detailed configuration settings for known, identified combinations of ports, protocols and services for enclave boundary defense

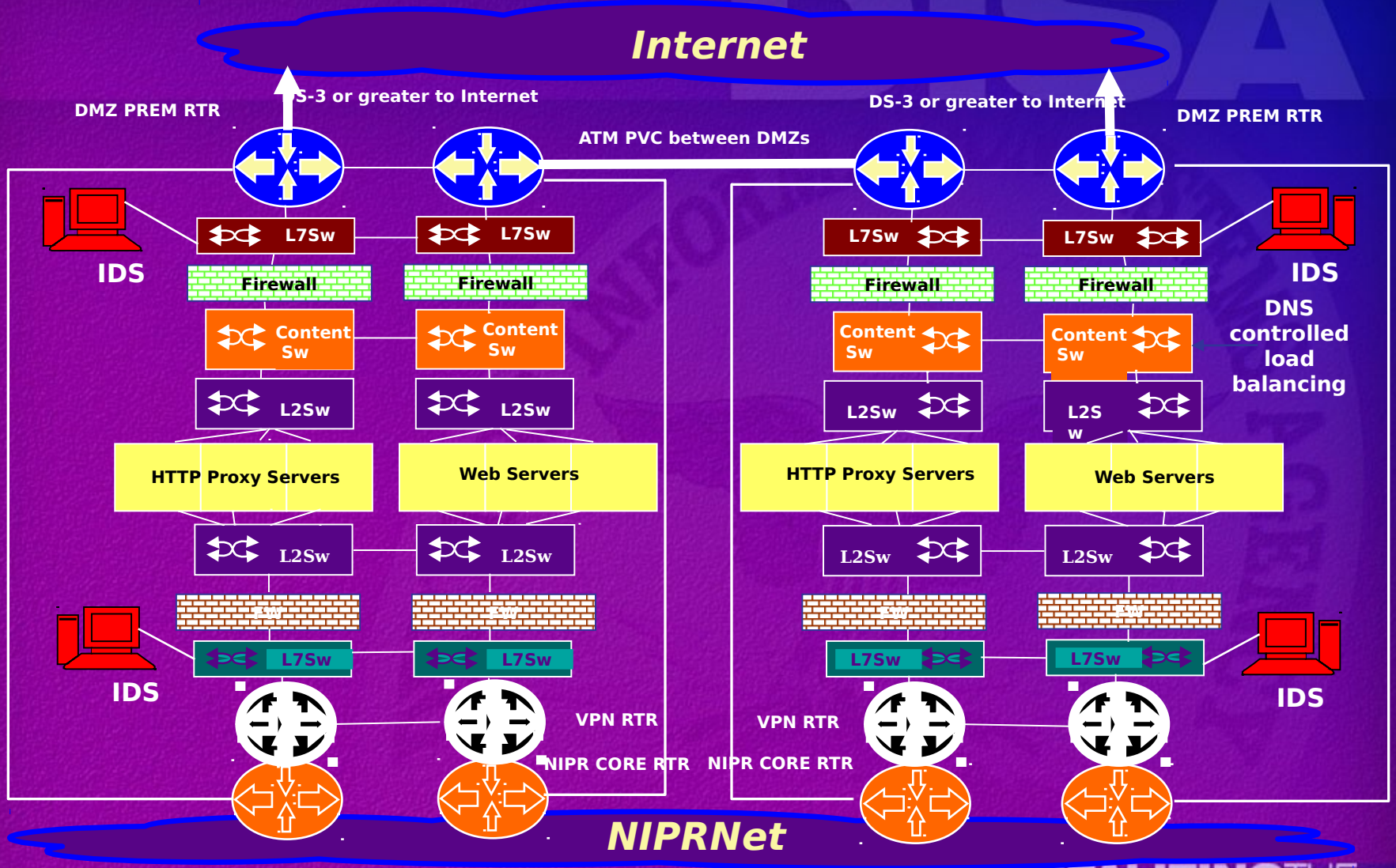
REALIZING THE NET-CENTRIC VISION

Web DMZ
DISA Technical Solution

- Supports Internet applications using Hyper Text Transfer Protocol (HTTP) / Secure HTTP (HTTPS)
- Domain Name Server (DNS) host name resolution
- Allows hosting of Critical DoD public web sites in DISA managed computing centers
- Securely accessible from “.com” environment

REALIZING THE NET-CENTRIC VISION

Redundant – Diverse - Virtual



REALIZING THE NET-CENTRIC VISION

B2B Requirements

- Approved mechanism for flexible Non-classified Internet Protocol Router Network (NIPRNet) connections when DoD policy requires services/protocols to be disconnected from Internet
- Authentication/access control within B2B Gateway
  - The primary communication links shall be secured via secure (IPSEC) VPN tunnels between the contractor's primary site and the B2B Gateway
- Layered security
  - Ports and protocols required by applications are encrypted from the source, decrypted and inspected in the DMZ, then proxied and re-encrypted for transmission to the application servers on the DISN
- Scalable to accommodate changing requirements
- Highly available (99.5%)

REALIZING THE NET-CENTRIC VISION

B2B Gateway Chronology

- MHS B2B Gateways
  - 4th QTR 2003, DISA MHS PO and TIMPO agree on architecture for MCSCs to access DoD hosted system thru B2B
  - 1st QTR 2004, 1st B2B in Columbus
  - 2nd QTR 2004, 2nd B2B in San Antonio
  - 2nd QTR 2004, IATO of “virtual” B2B
- DoD B2B Gateways
  - 2nd QTR 2004, agreement from DoD DMZ PO to fund additional B2Bs for general DoD use in San Antonio and Montgomery
  - 2nd QTR 2004, currently building acquisition package, developing CONOPs, modifying ATO submission paperwork

REALIZING THE NET-CENTRIC VISION

B2B Gateway
DISA Technical Solution

- Provides controlled and secure access
  - For defense contractors and other DoD partners to interconnect with non-Web based DOD government systems that reside on DOD networks
  - Uses various electronic devices for security, identification, authorization, and controlled access
- All contractor systems that will communicate with DoD systems will interconnect through the established B2B Gateway

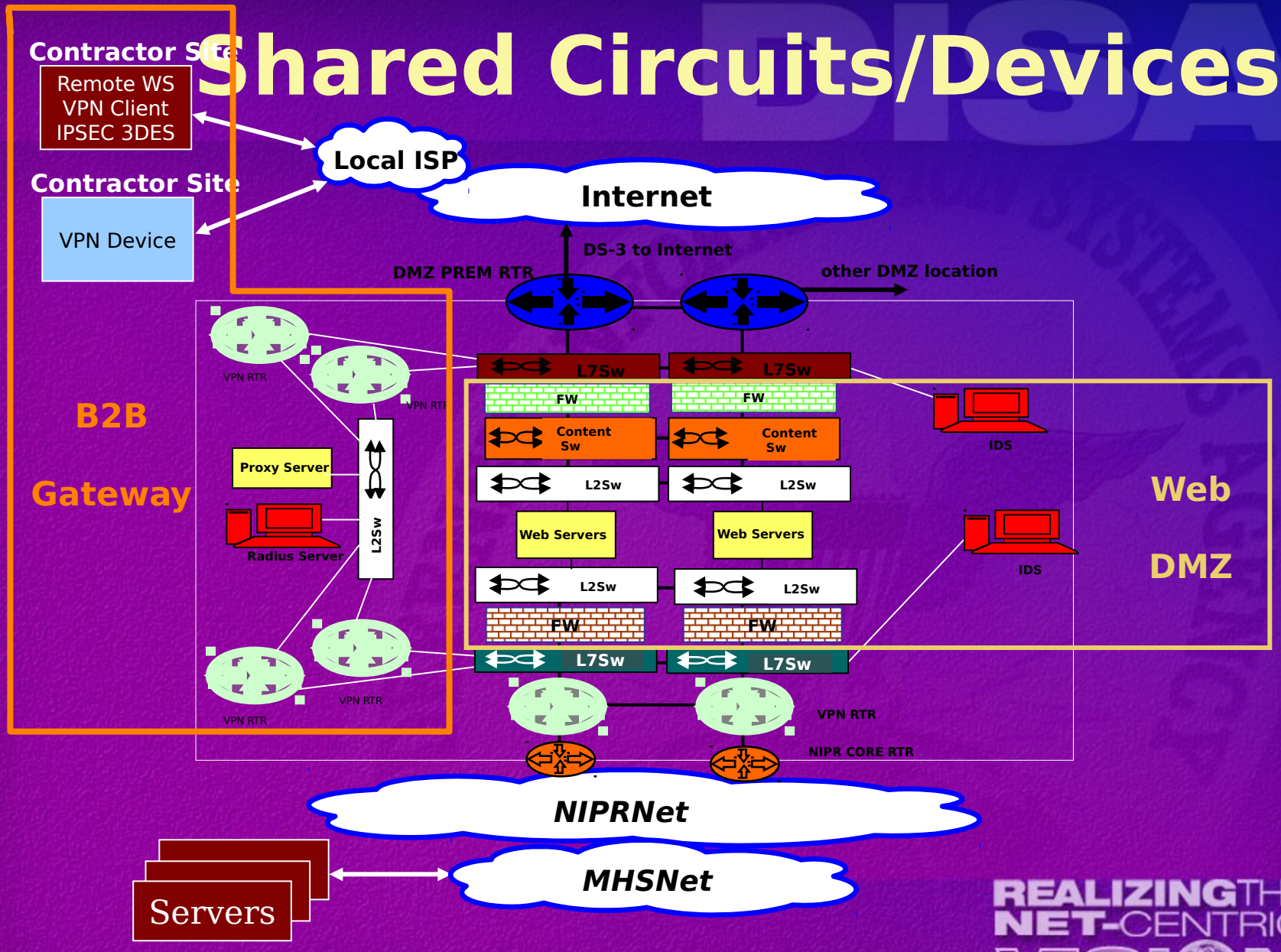
REALIZING THE NET-CENTRIC VISION

B2B Gateway
DISA Technical Solution

- B2B Gateway solution requires Government and Contractor VPNs
  - DISA uses Netscreen VPN at B2B Gateway
  - Contractors supply remote equipment
    - Must meet the Government's needs in facilitating remote management of VPN edge equipment with respect to access control, key management, and tunnel authentication.
- IPSEC tunnels – Supported by DISA with remote mgmt.
  - Site to site
  - Desktop software IPSEC clients supported
  - All tunnels must be authenticated

REALIZING THE NET-CENTRIC VISION

Shared Circuits/Devices



REALIZING THE NET-CENTRIC VISION

B2B/Web DMZ Security Features

- Web DMZ
  - Shared Security features with B2B Gateway
    - Intrusion Detection System
    - Firewall provides Internet screening
  - Content/Proxy servers protect Web server
  - Encryption via SSL/443
  - From arbitrary users at arbitrary locations to specific web addresses
- B2B
  - Encryption from user client to gateway
  - User application level authentication
  - Proxy services based on specific source and destination addresses for specific ports and protocols

REALIZING THE NET-CENTRIC VISION

DEFENSE INFORMATION SYSTEMS AGENCY